CyberSEA Research Lab
Carleton University
https://carleton.ca/cybersea/
@carleton-cybersea

Systems and Computer Engineering
Carleton University
1125 Colonel By Drive
Ottawa, ON K1S 5B6

Posting#: 2027-MASC-CDE-03

November 13, 2026

Position Available: M.A.Sc. Candidate

Modeling Cascading Cyberattack Impacts in Critical Systems

The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab at Carleton University is actively looking for a Master's student to work on a funded research project on the topic of modeling cascading cyberattack impacts in critical systems, starting in September 2027 or sooner.

Project Description and Objectives

Critical cyber-physical systems support essential services in areas such as healthcare, manufacturing, water treatment, energy, and transportation. These systems combine software, communication networks, physical processes, human operators, and organizational procedures. Because their components are interconnected, a cyberattack affecting one part of a system can produce consequences that spread far beyond the initially compromised component.

The full impact of a cyberattack may not be immediate or easy to predict. A small disruption can grow over time, interact with other system conditions, trigger feedback loops, or cascade across dependent components and services. For example, the loss of a monitoring function may initially appear manageable but could delay the detection of a physical process failure, interfere with operator decisions, and eventually cause a larger operational, safety, environmental, or economic consequence.

Many cybersecurity assessments provide a largely static view of impact. They describe the expected consequences of an attack at a particular point in time but may not adequately represent delayed effects, cumulative harm, feedback loops, nonlinear amplification, or cascading failures. This limitation can make it difficult to anticipate how a localized cyber disruption could develop into a sustained or system-wide failure.

The objective of this M.A.Sc. project is to develop and evaluate methods for modeling how cyberattack impacts evolve and cascade through critical cyber-physical systems over time. The research will investigate the relationships among initial cyber disruptions, system dependencies, physical processes, operational responses, and resulting consequences.

Project Keywords:

- cybersecurity
- cyber-physical systems
- cascading impacts
- temporal analysis
- modeling and simulation
- network science
- dynamic systems
- data analytics
- cyber resilience
- critical infrastructure

Duties and Responsibilities

The successful candidate will conduct research leading to an M.A.Sc. thesis and peer-reviewed publications. The anticipated research activities include:

1. Investigating existing approaches for modeling temporal, cumulative, and cascading consequences of cyberattacks in interconnected systems.
2. Developing models and methods for analyzing how cyberattack consequences emerge, evolve, and propagate through interconnected cyber and physical processes, including the effects of system dependencies, feedback mechanisms, and operating conditions.
3. Investigating and applying suitable analytical and simulation-based techniques for studying consequence propagation, including factors such as impact magnitude, duration, propagation speed, affected system scope, and recovery.
4. Designing and conducting simulation experiments to evaluate how different attack scenarios, system configurations, operating conditions, and mitigation strategies influence the development and propagation of consequences.
5. Applying and evaluating the proposed methods through critical cyber-physical system case studies, collaborating with other members of the research team, and communicating research results through scholarly publications and presentations.

Expected Research Contributions

The specific direction of the research will be refined with the successful candidate. Anticipated contributions include:

- Models and methods for representing and analyzing how cyberattack consequences emerge, evolve, and propagate over time, including cumulative and cascading effects.
- Analytical and simulation-based techniques for evaluating consequence propagation, considering factors such as impact magnitude, duration, affected system scope, and recovery.
- Methods and supporting tools for evaluating how system dependencies, operating conditions, and mitigation strategies influence the development and propagation of consequences.
- Empirical evidence and case studies demonstrating the applicability and practical value of the proposed methods for analyzing cyberattack consequences in critical cyber-physical systems.

Desired Skills/Qualifications

Suitable candidates will have a Bachelor's degree in Software Engineering, Computer Science, Computer Engineering, Systems Engineering, Cybersecurity, Applied Mathematics, Data Science, or a closely related field.

Ideal candidates will be self-motivated, intellectually curious, and able to work both independently and collaboratively. Candidates should have strong analytical and problem-solving abilities, effective written and oral communication skills, and an interest in conducting rigorous research with practical relevance.

Applicants should demonstrate preparation or interest in several of the following areas:

- modeling and simulation of complex systems;
- cybersecurity, security engineering, or cyber-physical systems;
- network science, graph theory, or systems analysis;
- dynamic systems, system dynamics, or discrete-event simulation;
- quantitative analysis, applied statistics, or data analytics; and
- system dependability, resilience, safety, or research software development.

Candidates should be comfortable reading and synthesizing technical literature, working with quantitative information, critically examining the assumptions and limitations of analytical measures, and clearly documenting research methods and decisions. Previous experience with cybersecurity projects, systematic or structured literature reviews, quantitative research, experimental design, data analysis, scientific software development, or scholarly writing will be considered an asset.

All candidates must satisfy the Minimum Admission Requirements for Doctoral Programs at Carleton University. International candidates must also ensure that they satisfy the English as a Second Language Requirements. In all cases, these requirements will be strictly enforced when evaluating an application for admission.

Funding

Successful candidates for this position will be *eligible for funding* in the form of a research assistantship. Specific funding details are determined at the time of offer and consider numerous factors such as academic standing, research potential, availability of funds, eligibility for teaching assistantship and/or scholarships, etc.

Research Training Environment

The successful candidate will join a collaborative research environment within the CyberSEA Research Lab, focused on identifying, measuring, and mitigating the consequences of cyberattacks on critical cyber-physical systems. The candidate will have opportunities to collaborate with other Master's and doctoral researchers working on related research projects and interdisciplinary problems.

The candidate will receive regular individual research supervision and participate in group meetings, research seminars, skills-development activities, and peer mentoring. Training and professional development will include research methodologies, technical skills relevant to the project, scientific writing, and the effective communication of research results.

The candidate will be encouraged and supported in publishing research at international conferences and in peer-reviewed journals, presenting at research and professional events, and developing the skills needed to conduct independent research and collaborate effectively within a research team.

Host Research Institute Information

Carleton University is a public comprehensive university, founded in 1942, in Ottawa, Ontario, Canada. The research-intensive Faculty of Engineering and Design at Carleton University is recognized as one of Canada's leading institutions in the study and research of engineering, architecture, industrial design and information technology. Since the inception of engineering at Carleton in 1945, our experts have pushed the bounds of innovation and discovery. Carleton focuses on anticipating the needs of industry and society, and offers forward-thinking programs with real world application and produces research that is helping to shape our present and future. The Department of Systems and Computer Engineering is a recognized world-class institution in software engineering, computer systems engineering, communications engineering, and biomedical engineering. Together with the Department of Electronics, the Department of Systems and Computer Engineering constitutes one of the largest and most research-intensive centres for Electrical and Computer Engineering and Software Engineering education and research in Canada. The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab conducts advanced academic research to develop systematic and rigorous approaches for evaluating and assuring the cyber security of software-dependent systems.

Further Information

For more information about Graduate Studies at Carleton University and the Department of Systems and Computer Engineering, please visit: https://carleton.ca/sce/graduate-studies/. For more information about applying for Graduate Studies at Carleton University, please visit: https://graduate.carleton.ca/apply-online/. For more information about funding for Graduate Studies, please visit: https://graduate.carleton.ca/financial-assistance/admissions-funding/.

Application Enquiries

Due to the high volume of generic and automated enquiries, only messages that explicitly identify an open position currently posted by the CyberSEA Research Lab and clearly explain how the applicant's background, experience, and research interests align with that position will be considered. Generic enquiries or messages that do not demonstrate a specific connection to the advertised project will not receive a response.

How to Apply

Interested applicants are to send a **CV** and **Statement of Interest** detailing your research interests, background, and experience by email to the CyberSEA Lab Director using the contact information below. Please include the specific **position posting number** in the subject line of your email.

Jason Jaskolka, Ph.D., P.Eng.
Systems and Computer Engineering | Carleton University
Canal Building 6206 | 1125 Colonel By Drive | Ottawa, ON K1S 5B6
jason.jaskolka@carleton.ca
https://carleton.ca/jaskolka/
@jason-jaskolka

For more information about how to apply, please visit: https://carleton.ca/cybersea/positions-available/

Application Deadline

Applications will be reviewed as they arrive until a suitable candidate is found.